

WHAT IS CLAIMED IS:

1. A method for facilitating a legal action relating to unsolicited electronic communication, the method comprising:

determining that a first entity is receiving unsolicited electronic communication;

obtaining first information associating a second entity with a source of at least a portion of the unsolicited electronic communication; and

obtaining second information sufficient to allow initiation of a legal action against the second entity relating to the unsolicited electronic communication.

2. The method of claim 1, comprising determining an impact of the unsolicited electronic communication on the first entity;

3. The method of claim 1, comprising determining that a first entity is receiving unsolicited electronic communication that comprises e-mail.

4. The method of claim 1, wherein the second information facilitates a method for facilitating a civil cause of action against the second entity.

5. The method of claim 1, further comprising determining an impact of the unsolicited electronic communication on the first entity by determining that damage has been suffered by the first entity due to the unsolicited electronic communication.

6. The method of claim 5, wherein determining the impact comprises at least one of calculating the impact, estimating the impact, quantifying the impact, and predicting the impact.
7. The method of claim 6, further comprising using statistical analysis to estimate the impact over a period of time.
8. The method of claim 1, wherein the first information indicates that the second entity is responsible for sending of the at least a portion of the unsolicited electronic communication.
9. The method of claim 1, wherein the first information indicates that the second entity is a source of at least a portion of the unsolicited electronic communication.
10. The method of claim 1, wherein the first and the second information is obtained in a forensically sound manner.
11. The method of claim 10, wherein the first and second information is obtained in a manner such that the first and the second information is useable as legal evidence to support the legal action.
12. The method of claim 1, wherein obtaining information sufficient to allow initiation of a

legal action against the second entity relating to the unsolicited electronic communication comprises storing copies of unsolicited e-mails received by the first entity in a secure database.

13. The method of claim 12, wherein the second information is obtained by unsolicited e-mails from a computer associated with the second entity through a secure channel to be stored in the secure database.

14. The method of claim 12, further comprising storing copies of the unsolicited e-mails in a knowledge database.

15. The method of claim 12, further comprising analyzing copies of the unsolicited e-mails using a parsing engine prior to storage in the knowledge database.

16. The method of claim 12, further comprising allowing querying of the knowledge database by the first entity.

17. The method of claim 14, further comprising storing unsolicited e-mails from a plurality of recipients including the first entity in the knowledge database.

18. The method of claim 17, further comprising using information stored in the knowledge database to facilitate at least one of identifying the second entity and determining the impact of

the unsolicited electronic communication.

19. The method of claim 17, further comprising identifying the second entity as being at least one of a spammer, a pirate, a hacker, and a virus sender.

20. The method of claim 1, further comprising using one or more email accounts to attract unsolicited e-mails.

21. The method of claim 20, further comprising storing in a knowledge database the unsolicited e-mails received by the one or more email accounts.

22. The method of claim 21, further comprising using the unsolicited e-mails received by the one or more email accounts to facilitate identification of one or more sources of the unsolicited e-mails.

23. The method of claim 1, wherein the unsolicited electronic communication comprises unsolicited e-mails, and wherein the second entity is responsible for sending at least a portion of the unsolicited e-mails.

24. The method of claim 23, further comprising utilizing the first information about the second entity to obtain third information about one or more additional entities, the additional entities

having communicated with the second entity and being responsible for sending unsolicited electronic communication.

25. The method of claim 24, wherein the second entity and the one or more additional entities communicated with each other via an electronic message board.

26. The method of claim 25, further comprising monitoring the electronic message board to obtain fourth information regarding communication between the second entity and the one or more additional entities.

27. The method of claim 24, further comprising identifying a potential target for a civil action from among the second entity and the one or more additional entities.

28. The method of claim 1, wherein the unsolicited electronic communication comprises e-mail, and wherein at least a first e-mail of the unsolicited e-mail comprises a reference to one or more URLs, and wherein opening the first e-mail causes a non-electronically formatted image to appear, and further comprising storing information about the first e-mail message in a secure database, the information comprising a copy of the first e-mail, each of the one or more URLs, and a copy of the image.

29. The method of claim 1, wherein the second information sufficient to allow a legal remedy

as a result of the legal action.

30. The method of claim 1, wherein the second information is sufficient to allow legal recovery comprising at least one of an injunction and damages as a result of the legal action.

31. A method of identifying senders of unsolicited e-mail, the method comprising:

- identifying an entity responsible for sending unsolicited e-mail;
- monitoring Internet activity by the entity;
- storing information relating to the Internet activity in a database;
- utilizing the stored information to identify other entities who are senders of unsolicited e-mail.

32. The method of claim 31, wherein identifying an entity comprises identifying a person, and wherein monitoring Internet activity comprises monitoring Internet activity by the person, and wherein utilizing stored information to identify other entities comprises utilizing stored information to identify other persons.

33. The method of claim 32, comprising utilizing the information in identifying potential targets of civil actions.

34. A method for facilitating bringing of a civil cause of action relating to sending of unsolicited e-mails, the method comprising:

determining that a first entity is receiving unsolicited e-mails;

determining an impact of the unsolicited e-mails on the first entity;

obtaining information evidencing that the second entity is at least partially responsible for sending at least a portion of the unsolicited e-mails; and

obtaining information sufficient to allow a legal action against the second entity relating to the unsolicited e-mails.

35. A system for facilitating a legal action relating to unsolicited electronic communication, the system comprising:

a network;

a server computer connected to the network;

a first computer connected to the network, the first computer being associated with a first entity; and

one or more databases connected with the server computer and the first computer;

wherein unsolicited electronic communication received by the first computer is sent to and stored in the one or more databases, and

wherein the server computer is effective in:

obtaining information associating a second entity with a source of at least a

portion of the unsolicited electronic communication; and

obtaining information sufficient to allow initiation of a legal action against the second entity relating to the unsolicited electronic communication.

36. The system of claim 35, wherein the one or more databases comprise one or more secure databases for securely storing copies of the unsolicited electronic communication.

37. The system of claim 36, wherein the one or more secure databases are used in storing information relating to unsolicited electronic communication in a forensically sound manner.

38. The system of claim 36, wherein the one or more databases further comprise one or more knowledge databases for storing copies of unsolicited electronic communication.

39. The system of claim 36, wherein the unsolicited electronic communication comprises e-mails, and the system further comprises a parsing engine effective to parse copies of the unsolicited electronic communication before storage in the one or more knowledge databases, and wherein the one or more knowledge databases comprise one or more relational databases that can be queried by the first entity.

40. A method for facilitating bringing a legal action against a second entity in relation to sending of unsolicited e-mails to a first entity, the method comprising:



utilizing one or more e-mail accounts to receive unsolicited e-mails;

sending unsolicited e-mails received by the one or more email accounts to one or more databases for storage;

analyzing information stored in the one or more databases and relating to the unsolicited e-mails to obtain information useful in facilitating bringing a legal action against one or more entities in relation with sending of the unsolicited e-mails to the first entity.

41. The method of claim 40, further comprising inducing harvesting of the e-mail account for use by senders of unsolicited e-mails.

42. The method of claim 40, further comprising utilizing a set of e-mail accounts and at least one Internet site to induce an internet spider to harvest at least a portion of the plurality of email accounts as if the email accounts were user e-mail accounts associated with an Internet Service Provider.

43. The method of claim 40, further comprising causing the one or more e-mail accounts to be listed on one or more "do not send" lists, so as to induce harvesting of the one or more e-mail accounts by an Internet spider for use by senders of unsolicited e-mails.

44. A method for facilitating bringing of a civil cause of action relating to sending of unsolicited e-mails, the method comprising:

determining that a first entity is receiving unsolicited e-mails;

obtaining first information evidencing that the second entity is at least partially responsible for sending at least a portion of the unsolicited e-mails; and

obtaining second information sufficient to allow a legal action against the second entity relating to the unsolicited electronic communication;

wherein a first e-mail of the unsolicited e-mails comprises a reference to one or more URLs, and wherein opening the first e-mail causes a non-electronically formatted image to appear, and wherein third information about the first e-mail message is stored in a secure database, the third information comprising a copy of the first e-mail, each of the one or more URLs, and a copy of the image.

45. The method of claim 44, further comprising determining an impact of the unsolicited e-mails on the first entity.

46. The method of claim 45, storing information about the image comprises storing information about a .GIF image.

47. A method for facilitating obtaining information regarding unsolicited e-mails, the method comprising:

one or more computers associated with a first entity sending copies of received unsolicited e-mails through a secure channel for storage in a secure database;

storing copies of the unsolicited e-mails in a knowledge database, the knowledge database being a relational database; and

allowing querying of the relational database to obtain information regarding the unsolicited e-mails.

48. The method of claim 47, comprising using information stored in the secure database in facilitating bringing a legal action against one or more entities determined to be at least partially responsible for sending at least a portion of the unsolicited e-mails.

49. The method of claim 47, comprising parsing the unsolicited e-mails before storage in the knowledge database.

50. The method of claim 47, comprising organizing information in the knowledge databases and relating to the unsolicited e-mails into tables.

51. A method for enabling action against a threat source, the method comprising:

receiving evidence relating to a plurality of unsolicited emails through a proprietary account and through a referral from a victim;

preserving the evidence in a secure evidence repository;

parsing the evidence to extract data relating to threat types, sources, intermediate parties, and beneficiaries, thereby producing parsed evidence;

correlating the parsed evidence to produce common threat types, sources, intermediaries, and beneficiaries relating to the unsolicited emails;

collecting information from both open and closed sources based on the correlating;

cross-referencing the information and the common threat types, sources, intermediaries, and beneficiaries; and

storing a result of the cross-referencing.

52. The method as recited in claim 51, further comprising:

querying the result for one of a threat source, beneficiary and intermediary thereby producing a query result with a threat type;

qualifying the threat type;

quantifying the threat type; and

producing a list of targets based on the qualifying and quantifying.

53. The method as recited in claim 52, further comprising:

querying intelligence relating to the list of targets;

reviewing information received from the intelligence; and

deciding whether to pursue action against one of the targets.